



2100 Pennsylvania Avenue, NW  
Washington, DC 20037-3213

T 202.293.7060  
F 202.293.7860

1010 El Camino Real  
Menlo Park, CA 94025-4345

T 650.325.5800  
F 650.325.6606

Toei Nishi Shimbashi Bldg. 4F  
13-5 Nishi Shimbashi 1-Chome  
Minato-Ku, Tokyo 105-0003  
Japan

T 03.3503.3760  
F 03.3503.3756

www.sughrue.com

Howard L. Bernstein  
T 202.663.7937  
hbernstein@sughrue.com

August 31, 2001

BOX PATENT APPLICATION  
Commissioner for Patents  
Washington, D.C. 20231

Re: Application of Takuya MORISHITA  
SYSTEM AND METHOD FOR DECRYPTING ENCRYPTED COMPUTER  
PROGRAM  
Assignee: NEC CORPORATION  
Our Ref. Q66052



Dear Sir:

Attached hereto is the application identified above including 13 sheets of the specification, including the claims and abstract, 4 sheets of drawings, executed Assignment and PTO 1595 form, and executed Declaration and Power of Attorney. Also enclosed is the Information Disclosure Statement.

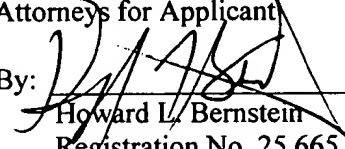
The Government filing fee is calculated as follows:

Total claims	<u>16</u> - 20	=	<u>          </u>	x	\$18.00	=	<u>          </u>	\$0.00
Independent claims	<u>4</u> - 3	=	<u>1</u>	x	\$80.00	=	<u>          </u>	\$80.00
Base Fee								\$710.00
<b>TOTAL FILING FEE</b>								<b>\$790.00</b>
Recordation of Assignment								\$40.00
<b>TOTAL FEE</b>								<b>\$830.00</b>

A check for the statutory filing fee of \$790.00 is attached. You are also directed and authorized to charge or credit any difference or overpayment to Deposit Account No. 19-4880. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16 and 1.17 and any petitions for extension of time under 37 C.F.R. § 1.136 which may be required during the entire pendency of the application to Deposit Account No. 19-4880. A duplicate copy of this transmittal letter is attached.

Priority is claimed from September 06, 2000 based on JP Application No. 2000-269460. The priority document is enclosed herewith.

Respectfully submitted,  
SUGHRUE, MION, ZINN,  
MACPEAK & SEAS, PLLC  
Attorneys for Applicant

By:   
Howard L. Bernstein  
Registration No. 25,665

MORISHITA #2  
Q 66052  
8/31/01  
10f1

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日  
Date of Application:

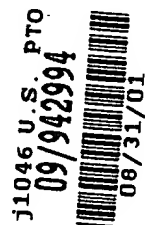
2000年 9月 6日

出 願 番 号  
Application Number:

特願2000-269460

出 願 人  
Applicant(s):

日本電気株式会社

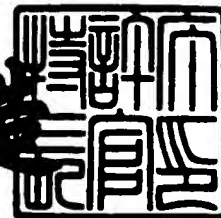


CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 5月25日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 68501855

【提出日】 平成12年 9月 6日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/06

【発明者】

    【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

    【氏名】 森下 卓也

【特許出願人】

    【識別番号】 000004237

    【氏名又は名称】 日本電気株式会社

【代理人】

    【識別番号】 100088812

    【弁理士】

    【氏名又は名称】 ▲柳▼川 信

【手数料の表示】

    【予納台帳番号】 030982

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 プログラムコードの不正改竄防止システム及びその方法並びにその制御プログラムを記録した記録媒体

【特許請求の範囲】

【請求項 1】 読込まれる暗号化プログラムを平文化するための暗号鍵を生成する暗号鍵算出手段と、前記暗号鍵算出手段で算出された暗号鍵を使用して前記暗号化プログラムの暗号を解除する暗号解除手段とを含むプログラムコードの不正改竄防止システムであって、前記暗号鍵算出手段が算出した暗号鍵を使用して前記暗号化プログラムの暗号を解除しかつ前記暗号解除手段よりも高速に暗号解除を実行する高速暗号解除手段を有し、自システムの初期化処理時に前記暗号解除手段で前記暗号化プログラムの暗号を解除し、自システムの実行処理時に前記高速暗号解除手段で前記暗号化プログラムの暗号を解除するようにしたことを特徴とするプログラムコードの不正改竄防止システム。

【請求項 2】 少なくともソフトウェアデバッガによってプログラムコードの動作を解析する不正操作が行われていないかどうかを検出する不正操作検出手段を含むことを特徴とする請求項 1 記載のプログラムコードの不正改竄防止システム。

【請求項 3】 前記暗号化プログラムは、実行しても意味の無い暗号化されたダミープログラムコードを含むこと特徴とする請求項 1 または請求項 2 記載のプログラムコードの不正改竄防止システム。

【請求項 4】 前記不正操作検出手段が前記不正操作を検出した時に前記ダミープログラムコードの暗号を解除するようにしたこと特徴とする請求項 3 記載のプログラムコードの不正改竄防止システム。

【請求項 5】 前記不正操作検出手段が前記不正操作を検出した時に前記暗号化プログラムの暗号解除処理を中止するようにしたこと特徴とする請求項 3 または請求項 4 記載のプログラムコードの不正改竄防止システム。

【請求項 6】 読込まれる暗号化プログラムを平文化するための暗号鍵を生成する暗号鍵算出手段と、前記暗号鍵算出手段で算出された暗号鍵を使用して前

記暗号化プログラムの暗号を解除する暗号解除手段とを含むプログラムコードの不正改竄防止システムの不正改竄防止方法であって、自システムの初期化処理時に前記暗号解除手段で前記暗号化プログラムの暗号を解除するステップと、自システムの実行処理時に前記暗号鍵算出手段が算出した暗号鍵を使用して前記暗号化プログラムの暗号を解除しかつ前記暗号解除手段よりも高速に暗号解除を実行する高速暗号解除手段で前記暗号化プログラムの暗号を解除するステップとを有することを特徴とするプログラムコードの不正改竄防止方法。

【請求項 7】 少なくともソフトウェアデバッガによってプログラムコードの動作を解析する不正操作が行われていないかどうかを検出するステップを含むことを特徴とする請求項 6 記載のプログラムコードの不正改竄防止方法。

【請求項 8】 前記暗号化プログラムは、実行しても意味の無い暗号化されたダミープログラムコードを含むこと特徴とする請求項 6 または請求項 7 記載のプログラムコードの不正改竄防止方法。

【請求項 9】 前記不正操作が行われていないかどうかを検出するステップが前記不正操作を検出した時に前記ダミープログラムコードの暗号を解除するようにしたこと特徴とする請求項 8 記載のプログラムコードの不正改竄防止方法。

【請求項 10】 前記不正操作が行われていないかどうかを検出するステップが前記不正操作を検出した時に前記暗号化プログラムの暗号解除処理を中止するようにしたこと特徴とする請求項 8 または請求項 9 記載のプログラムコードの不正改竄防止方法。

【請求項 11】 読込まれる暗号化プログラムを平文化するための暗号鍵を生成する暗号鍵算出手段と、前記暗号鍵算出手段で算出された暗号鍵を使用して前記暗号化プログラムの暗号を解除する暗号解除手段とを含むプログラムコードの不正改竄防止システムの不正改竄防止制御プログラムを記録した記録媒体であって、前記不正改竄防止制御プログラムは前記暗号化プログラムを実行するデータ処理装置に、自装置の初期化処理時に前記暗号解除手段で前記暗号化プログラムの暗号を解除させ、自装置の実行処理時に前記暗号鍵算出手段が算出した暗号鍵を使用して前記暗号化プログラムの暗号を解除しかつ前記暗号解除手段よりも高速に暗号解除を実行する高速暗号解除手段で前記暗号化プログラムの暗号を解

除させることを特徴とするプログラムコードの不正改竄防止制御プログラムを記録した記録媒体。

【請求項 1 2】 前記不正改竄防止制御プログラムは前記データ処理装置に、少なくともソフトウェアデバッガによってプログラムコードの動作を解析する不正操作が行われていないかどうかを検出させることを特徴とする請求項 1 1 記載のプログラムコードの不正改竄防止制御プログラムを記録した記録媒体。

【請求項 1 3】 前記不正改竄防止制御プログラムは前記データ処理装置に、前記不正操作が行われていないかどうかを検出させる際に、前記不正操作が検出された時に前記暗号化プログラムに含まれかつ実行しても意味の無い暗号化されたダミープログラムコードの暗号を解除させること特徴とする請求項 1 2 記載のプログラムコードの不正改竄防止制御プログラムを記録した記録媒体。

【請求項 1 4】 前記不正改竄防止制御プログラムは前記データ処理装置に、前記不正操作が行われていないかどうかを検出させる際に、前記不正操作が検出された時に前記暗号化プログラムの暗号解除処理を中止させること特徴とする請求項 1 2 または請求項 1 3 記載のプログラムコードの不正改竄防止制御プログラムを記録した記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明はプログラムコードの不正改竄防止システム及びその方法並びにその制御プログラムを記録した記録媒体に関し、特にプログラムコードに対して暗号化を施してその不正改竄を防止するシステムに関する。

【0 0 0 2】

【従来の技術】

従来、プログラムコードの不正改竄防止システムとしては、特開 2 0 0 0 - 1 2 2 8 6 1 号公報に開示されたシステムがある。この不正改竄防止システムは、図 4 に示すように、プログラム制御によって動作するデータ処理装置 3 と、ファイル装置 4 とから構成されている。

【0 0 0 3】

データ処理装置 3 は非暗号プログラム読込み手段 3 1 と、暗号鍵算出手段 3 2 と、暗号化プログラム読込み手段 3 3 と、暗号解除手段 3 4 とからなり、ファイル装置 4 は非暗号プログラム記憶手段 4 1 と、暗号化プログラム記憶手段 4 2 とからなる。

## 【0 0 0 4】

上記のプログラムコードの不正改竄防止システムにおいて、非暗号プログラム記憶手段 4 1 には暗号化されていないプログラムコードが格納され、暗号化プログラム記憶手段 4 2 には暗号化されたプログラムコード # 1 ~ # n が複数のブロック # 1 ~ # n にそれぞれ分割されて格納されている。これらは非暗号プログラム記憶手段 4 1 に格納された暗号化されていないプログラムコード、暗号化されたブロック # 1 ~ # n の順に、データ処理装置 3 に読込まれるものとする。

## 【0 0 0 5】

非暗号プログラム読込み手段 3 1 は非暗号プログラム記憶手段 4 1 から図示せぬ主記憶上に暗号化されていないプログラムコードを読込む。暗号鍵算出手段 3 2 はこの主記憶上にあるプログラムコードの一方向関数（ハッシュ関数等）を使用し、読込まれる暗号化されたプログラムコードブロックを平文化するための暗号鍵を生成する。

## 【0 0 0 6】

暗号化プログラム読込み手段 3 3 は暗号化プログラム記憶手段 4 2 から主記憶上に次に実行する暗号化されたプログラムコードを読込む。暗号解除手段 3 4 は暗号鍵算出手段 3 2 で算出された暗号鍵を使用し、暗号化されたプログラムコードの暗号を解除する。

## 【0 0 0 7】

## 【発明が解決しようとする課題】

上述した従来のプログラムコードの不正改竄防止システムでは、上記のようなプログラムコードの暗号解除処理を繰り返すため、暗号化が施されたプログラムコードを実行する際の実行速度が、プログラムコードに暗号化を施さない場合と比較して遅くなるという問題がある。

## 【0 0 0 8】

また、従来のプログラムコードの不正改竄防止システムでは、ソフトウェアデバグ等のプログラムコードを実行しながら解析する手段に対して対策を行っていないため、プログラムコードの暗号を解除する際に使用する暗号鍵を不正な方法で使用者に取得される可能性があるという問題がある。

【 0 0 0 9 】

そこで、本発明の目的は上記の問題点を解消し、暗号化されたプログラムコードを高速に実行することができるプログラムコードの不正改竄防止システム及びその方法並びにその制御プログラムを記録した記録媒体を提供することにある。

【 0 0 1 0 】

また、本発明の他の目的は、プログラムコードの暗号を解除する際に使用する暗号鍵を不正な方法で使用者に取得される可能性を低くすることができるプログラムコードの不正改竄防止システム及びその方法並びにその制御プログラムを記録した記録媒体を提供することにある。

【 0 0 1 1 】

【課題を解決するための手段】

本発明によるプログラムコードの不正改竄防止システムは、読込まれる暗号化プログラムを平文化するための暗号鍵を生成する暗号鍵算出手段と、前記暗号鍵算出手段で算出された暗号鍵を使用して前記暗号化プログラムの暗号を解除する暗号解除手段とを含むプログラムコードの不正改竄防止システムであって、前記暗号鍵算出手段が算出した暗号鍵を使用して前記暗号化プログラムの暗号を解除しかつ前記暗号解除手段よりも高速に暗号解除を実行する高速暗号解除手段を備え、自システムの初期化处理時に前記暗号解除手段で前記暗号化プログラムの暗号を解除し、自システムの実行処理時に前記高速暗号解除手段で前記暗号化プログラムの暗号を解除するようにしている。

【 0 0 1 2 】

本発明による他のプログラムコードの不正改竄防止システムは、上記の構成のほかに、少なくともソフトウェアデバグによってプログラムコードの動作を解析する不正操作が行われていないかどうかを検出する不正操作検出手段を具備している。



## 【 0 0 1 3 】

本発明によるプログラムコードの不正改竄防止方法は、読込まれる暗号化プログラムを平文化するための暗号鍵を生成する暗号鍵算出手段と、前記暗号鍵算出手段で算出された暗号鍵を使用して前記暗号化プログラムの暗号を解除する暗号解除手段とを含むプログラムコードの不正改竄防止システムの不正改竄防止方法であって、自システムの初期化処理時に前記暗号解除手段で前記暗号化プログラムの暗号を解除するステップと、自システムの実行処理時に前記暗号鍵算出手段が算出した暗号鍵を使用して前記暗号化プログラムの暗号を解除しかつ前記暗号解除手段よりも高速に暗号解除を実行する高速暗号解除手段で前記暗号化プログラムの暗号を解除するステップとを備えている。

## 【 0 0 1 4 】

本発明による他のプログラムコードの不正改竄防止方法は、上記のステップのほかに、少なくともソフトウェアデバッガによってプログラムコードの動作を解析する不正操作が行われていないかどうかを検出するステップを具備している。

## 【 0 0 1 5 】

本発明によるプログラムコードの不正改竄防止制御プログラムを記録した記録媒体は、読込まれる暗号化プログラムを平文化するための暗号鍵を生成する暗号鍵算出手段と、前記暗号鍵算出手段で算出された暗号鍵を使用して前記暗号化プログラムの暗号を解除する暗号解除手段とを含むプログラムコードの不正改竄防止システムの不正改竄防止制御プログラムを記録した記録媒体であって、前記不正改竄防止制御プログラムは前記暗号化プログラムを実行するデータ処理装置に、自装置の初期化処理時に前記暗号解除手段で前記暗号化プログラムの暗号を解除させ、自装置の実行処理時に前記暗号鍵算出手段が算出した暗号鍵を使用して前記暗号化プログラムの暗号を解除しかつ前記暗号解除手段よりも高速に暗号解除を実行する高速暗号解除手段で前記暗号化プログラムの暗号を解除させている。

## 【 0 0 1 6 】

本発明による他のプログラムコードの不正改竄防止制御プログラムを記録した記録媒体は、上記の動作のほかに、前記不正改竄防止制御プログラムは前記デー

タ処理装置に、少なくともソフトウェアデバッガによってプログラムコードの動作を解析する不正操作が行われていないかどうかを検出させている。

## 【 0 0 1 7 】

すなわち、本発明のプログラムコードの不正改竄防止システムは、暗号化されたプログラムコードを高速に実行し、さらにソフトウェアデバッガ等による解析を困難にすることが可能な構成を提供するものである。

## 【 0 0 1 8 】

より具体的に、本発明のプログラムコードの不正改竄防止システムでは、暗号解除手段と同様に、暗号鍵算出手段が算出した暗号鍵を使用して暗号化されたプログラムコードの暗号を解除するが、暗号解除手段よりも高速に暗号解除を実行する高速暗号解除手段と、ソフトウェアデバッガ等によってプログラムコードの動作が解析されていないかどうかを検出する不正操作検出手段とを有している。

## 【 0 0 1 9 】

本発明のプログラムコードの不正改竄防止システムでは、不正操作検出手段がプログラムコードの解析が行われていると判定した場合、以降の処理で暗号化されたプログラムコードを使用せずに暗号化されたダミープログラムを使用するかあるいは処理を中止する。

## 【 0 0 2 0 】

このように動作させることで、本発明のプログラムコードの不正改竄防止システムでは、暗号化されたプログラムコードを高速に実行し、さらにソフトウェアデバッガ等による解析を困難にすることができる構成を可能にする。

## 【 0 0 2 1 】

## 【発明の実施の形態】

次に、本発明の一実施例について図面を参照して説明する。図 1 は本発明の一実施例によるプログラムコードの不正改竄防止システムの構成を示すブロック図である。図 1 において、プログラムコードの不正改竄防止システムはプログラム制御によって動作するデータ処理装置 1 と、ファイル装置 2 とから構成されている。

## 【 0 0 2 2 】

データ処理装置 1 は非暗号プログラム読込み手段 1 1 と、暗号鍵算出手段 1 2 と、暗号化プログラム読込み手段 1 3 と、暗号解除手段 1 4 と、不正操作検出手段 1 5 と、高速暗号解除手段 1 6 とから構成されている。また、ファイル装置 2 は非暗号プログラム記憶手段 2 1 と、暗号化プログラム記憶手段 2 2 とから構成されている。

## 【 0 0 2 3 】

ファイル装置 2 において、非暗号プログラム記憶手段 2 1 には暗号化されていないプログラムコード（以下、非暗号プログラムとする）が格納され、暗号化プログラム記憶手段 2 2 には暗号化されたプログラムコード（以下、暗号化プログラムとする）# 1 ～ # n が複数のブロック # 1 ～ # n にそれぞれ分割されて格納されている。これらは非暗号プログラム、ブロック # 1 ～ # n の暗号化プログラムの順に、データ処理装置 1 に読込まれるものとする。

## 【 0 0 2 4 】

また、暗号化プログラム記憶手段 2 2 の各ブロック # 1 ～ # n は予め一つ前に実行されるプログラムコードから暗号鍵算出手段 1 2 が算出した暗号鍵で暗号化されている。さらに、暗号化プログラム記憶手段 2 2 の全ブロック # 1 ～ # n はまとめて予め非暗号プログラム記憶手段 2 1 に格納されたプログラムコードから暗号鍵算出手段 1 2 が算出した暗号鍵で暗号化されている。

## 【 0 0 2 5 】

暗号化プログラム記憶手段 2 2 には暗号化されたダミープログラムコード（以下、暗号化ダミープログラムとする）も格納されている。暗号化ダミープログラムは実行しても意味の無いプログラムコードであり、本来実行されるプログラムコードと同様に、複数のブロック # 1 ～ # n に分割されて格納されている。

## 【 0 0 2 6 】

非暗号プログラム読込み手段 1 1 は非暗号プログラム記憶手段 2 1 から図示せぬ主記憶上に非暗号プログラムを読込む。暗号鍵算出手段 1 2 はこの主記憶上にあるプログラムコードの一方向関数（ハッシュ関数等）を使用し、読込まれる暗号化プログラムを平文化するための暗号鍵を生成する。

## 【 0 0 2 7 】

暗号化プログラム読込み手段 1 3 は暗号化プログラム記憶手段 2 2 から主記憶上に次に実行する暗号化プログラムを読込む。暗号解除手段 1 4 は暗号鍵算出手段 1 2 で算出された暗号鍵を使用し、暗号化プログラムの暗号を解除する。

## 【 0 0 2 8 】

不正操作検出手段 1 5 はソフトウェアデバッガ等によってプログラムコードの動作が解析されていないかどうかを検出する。高速暗号解除手段 1 6 は、暗号解除手段 1 4 と同様に、暗号鍵算出手段 1 2 で算出された暗号鍵を使用し、暗号化プログラムの暗号を解除するが、暗号解除手段 1 4 より高速に暗号解除を実行するようになっている。

## 【 0 0 2 9 】

図 2 は本発明の一実施例によるプログラムコードの不正改竄防止システムの初期化時の動作を示すフローチャートであり、図 3 は本発明の一実施例によるプログラムコードの不正改竄防止システムの実行時の動作を示すフローチャートである。これら図 1 ～図 3 を参照して本発明の一実施例によるプログラムコードの不正改竄防止システム全体の動作について説明する。尚、図 2 及び図 3 に示す動作はデータ処理装置 1 が図示せぬ制御メモリに記録されたプログラムを実行することで実現され、制御メモリとしては R O M（リードオンリメモリ）やフロッピディスク等が使用可能である。

## 【 0 0 3 0 】

本発明の一実施例によるプログラムコードの不正改竄防止システムの動作は大きく分けて初期化時の動作と実行時の動作とに分かれている。初期化時の動作は図 2 に、実行時の動作は図 3 にそれぞれ示されている。初期化時の処理は一度しか実行されないが、実行時の処理は暗号化プログラムの実行を必要とする毎に実行される。

## 【 0 0 3 1 】

まず、データ処理装置 1 の初期化時において、非暗号プログラム読込み手段 1 1 は非暗号プログラム記憶手段 2 1 から非暗号プログラムを主記憶上に読込み、プログラムコードの実行を開始する（図 2 ステップ S 1）。通常、この処理はオペレーティングシステムのプログラム実行機構（図示せず）で管理されている。

## 【 0 0 3 2 】

不正操作検出手段 1 5 はソフトウェアデバッガ等によってプログラムコードの動作が解析されていないかどうかを検出する（図 2 ステップ S 2）。動作解析等の不正操作が行われていない場合、暗号鍵算出手段 1 0 2 は非暗号プログラム読み込み手段 1 1 が主記憶上に読込んだプログラムコードをハッシュ関数等の一方向関数で変換し、暗号鍵を生成する（図 2 ステップ S 3）。

## 【 0 0 3 3 】

暗号化プログラム読み込み手段 1 3 は暗号化プログラム記憶手段 2 2 から主記憶上に暗号化プログラムの全ブロックを読込む（図 2 ステップ S 4）。暗号解除手段 1 4 は暗号鍵算出手段 1 2 で算出された暗号鍵を使用し、暗号化プログラムの暗号を解除する（図 2 ステップ S 5）。但し、この段階では暗号化プログラムの暗号は全て解除されず、後に各ブロック毎に高速暗号解除手段 1 6 で再度暗号を解除する必要がある。不正操作が行われていない場合の初期化時の処理は以上で終了する。

## 【 0 0 3 4 】

不正操作が行われている場合、暗号鍵算出手段 1 2 は非暗号プログラム読み込み手段 1 1 が主記憶上に読込んだプログラムコードをハッシュ関数等の一方向関数で変換し、暗号化ダミープログラムの暗号を解除する暗号鍵を生成する（図 2 ステップ S 6）。

## 【 0 0 3 5 】

暗号化プログラム読み込み手段 1 3 は暗号化プログラム記憶手段 2 2 から主記憶上に暗号化ダミープログラムの全ブロックを読込む（図 2 ステップ S 7）。暗号解除手段 1 4 は暗号鍵算出手段 1 2 で算出された暗号鍵を使用し、暗号化ダミープログラムの暗号を解除する（図 2 ステップ S 8）。但し、この段階では暗号化ダミープログラムの暗号は全て解除されず、後に各ブロック毎に高速暗号解除手段 1 6 で再度暗号を解除する必要がある。

## 【 0 0 3 6 】

しかしながら、この暗号解除で得られるプログラムコードはダミーコードのため、実際に実行されるはずの処理は一切行われず、不正操作が行われていた場

合の初期化時の処理は以上で終了する。

【 0 0 3 7 】

一方、データ処理装置 1 の実行時において、不正操作検出手段 1 5 はソフトウェアデバッガ等によってプログラムコードの動作が解析されていないかどうかを検出する（図 3 ステップ S 1 1）。データ処理装置 1 は不正操作が行われている場合、その実行時の処理を終了する。

【 0 0 3 8 】

動作解析等の不正操作が行われていない場合、高速暗号解除手段 1 6 は暗号化プログラムを 1 ブロック主記憶上で複写する（図 3 ステップ S 1 2）。高速暗号解除手段 1 6 は複写された主記憶上の暗号化プログラムを暗号鍵算出手段 1 2 で算出された暗号鍵を使用して暗号を解除する（図 3 ステップ S 1 3）。

【 0 0 3 9 】

この時、高速暗号解除手段 1 6 による暗号解除は暗号解除手段 1 4 よりも高速に実行される。高速な暗号解除としては、例えば暗号鍵長を短くしたり、あるいはラウンド数を減らしたりすることで容易に実現可能である。

【 0 0 4 0 】

暗号鍵算出手段 1 2 は暗号解除されたプログラムコードのハッシュ値を算出し、これを次回の暗号解除時の暗号鍵とする（図 3 ステップ S 1 4）。この後に、データ処理装置 1 は現在主記憶上にある暗号が解除されたプログラムコードを実行する（図 3 ステップ S 1 5）。この処理の中では不正コピーの判定等が行われる。

【 0 0 4 1 】

続いて、データ処理装置 1 は現在主記憶上にある暗号が解除されたプログラムコードを破棄する（図 3 ステップ S 1 6）。データ処理装置 1 は暗号化プログラム記憶手段 2 2 内の全てのブロックのプログラムコードについて上記の処理が行われたかどうかを判定し（図 3 ステップ S 1 7）、全てのブロックのプログラムコードについて処理が実行されていれば処理を終了し、全てのブロックのプログラムコードについて処理が実行されていない場合はステップ S 1 1 に戻って処理が継続される。

【 0 0 4 2 】

このように、暗号化処理を一度しか実行しない初期化処理と複数回実行される実行処理とに分離し、実行処理に使用する暗号解除アルゴリズムに高速なものを使用することによって、暗号化プログラムを高速に実行することができる。

【 0 0 4 3 】

また、ソフトウェアデバッガ等のプログラムコードを実行しながら動作を解析する手段を検出した時にその後の動作を変えることによって、正しい暗号鍵を得ることを困難にすることができるので、プログラムコードの暗号を解除する際に使用する暗号鍵を不正な方法で使用者に取得される可能性を低くすることができる。

【 0 0 4 4 】

【発明の効果】

以上説明したように本発明のプログラムコードの不正改竄防止システムによれば、読込まれる暗号化プログラムを平文化するための暗号鍵を生成する暗号鍵算出手段と、暗号鍵算出手段で算出された暗号鍵を使用して暗号化プログラムの暗号を解除する暗号解除手段とを含むプログラムコードの不正改竄防止システムにおいて、自システムの初期化処理時に暗号解除手段で暗号化プログラムの暗号を解除し、自システムの実行処理時に暗号鍵算出手段が算出した暗号鍵を使用して暗号化プログラムの暗号を解除しかつ暗号解除手段よりも高速に暗号解除を実行する高速暗号解除手段で暗号化プログラムの暗号を解除することによって、暗号化されたプログラムコードを高速に実行することができるという効果がある。

【 0 0 4 5 】

また、本発明の他のプログラムコードの不正改竄防止システムによれば、少なくともソフトウェアデバッガによってプログラムコードの動作を解析する不正操作が行われていないかどうかを検出することによって、プログラムコードの暗号を解除する際に使用する暗号鍵を不正な方法で使用者に取得される可能性を低くすることができるという効果がある。

【図面の簡単な説明】

【図 1】

本発明の一実施例によるプログラムコードの不正改竄防止システムの構成を示すブロック図である。

【図 2】

本発明の一実施例によるプログラムコードの不正改竄防止システムの初期化時の動作を示すフローチャートである。

【図 3】

本発明の一実施例によるプログラムコードの不正改竄防止システムの実行時の動作を示すフローチャートである。

【図 4】

従来例によるプログラムコードの不正改竄防止システムの構成を示すブロック図である。

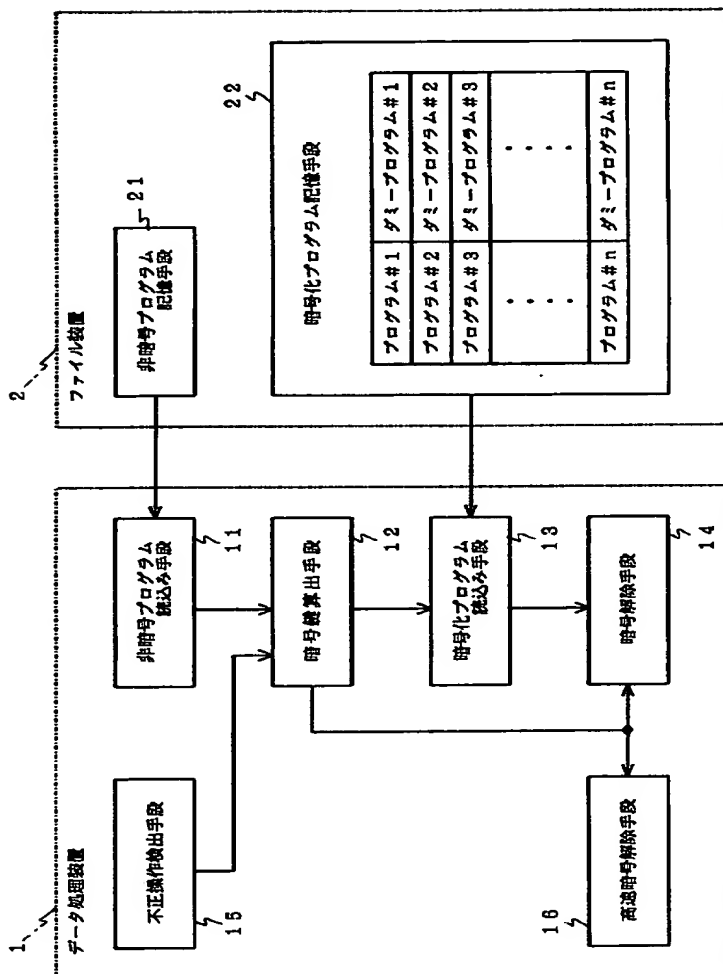
【符号の説明】

- 1   データ処理装置
- 2   ファイル装置
- 1 1   非暗号プログラム読み込み手段
- 1 2   暗号鍵算出手段
- 1 3   暗号化プログラム読み込み手段
- 1 4   暗号解除手段
- 1 5   不正操作検出手段
- 1 6   高速暗号解除手段
- 2 1   非暗号プログラム記憶手段
- 2 2   暗号化プログラム記憶手段

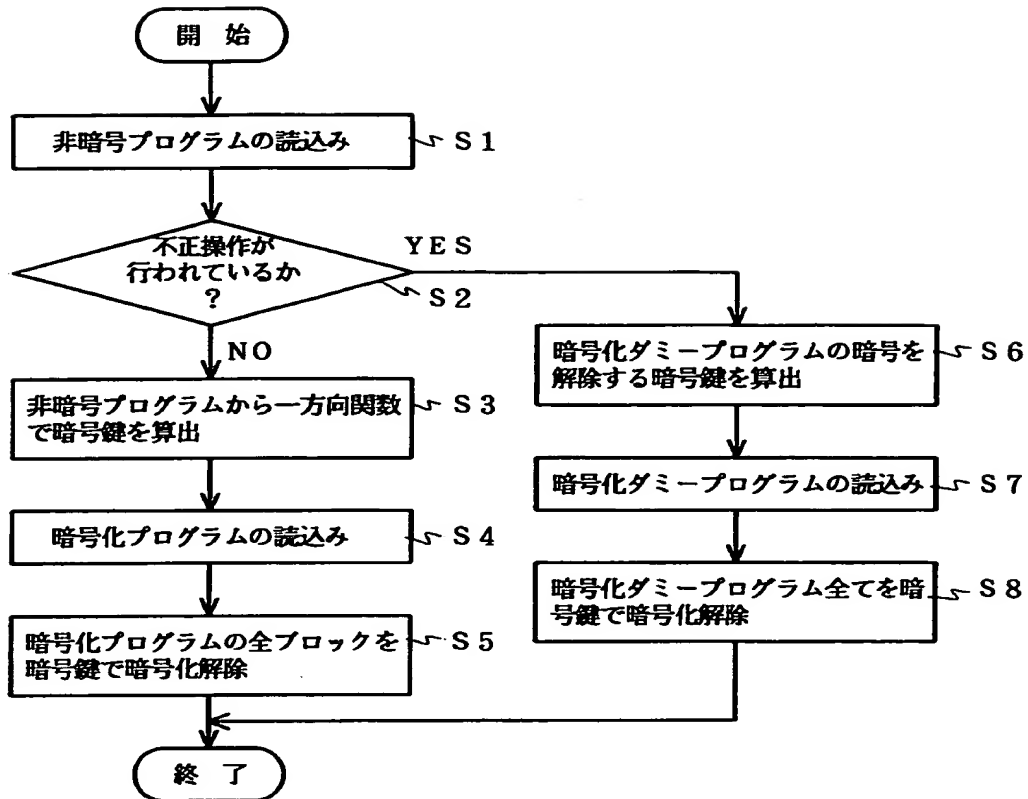


【書類名】 図面

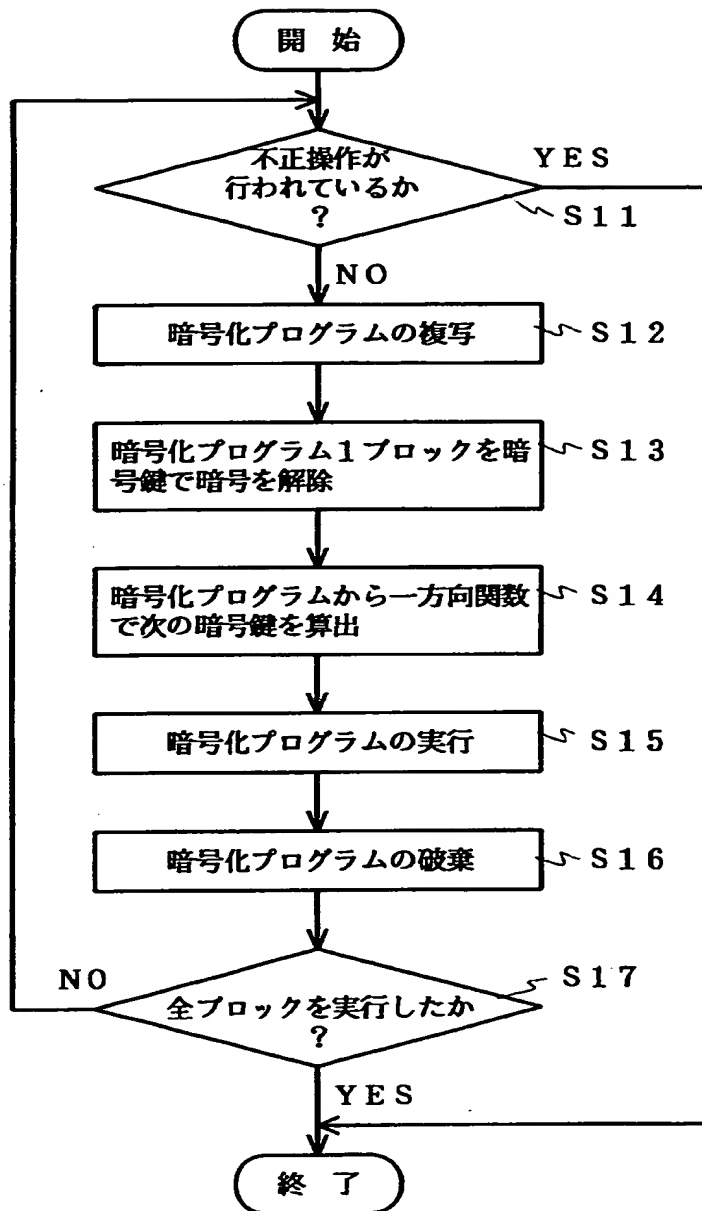
【図 1】



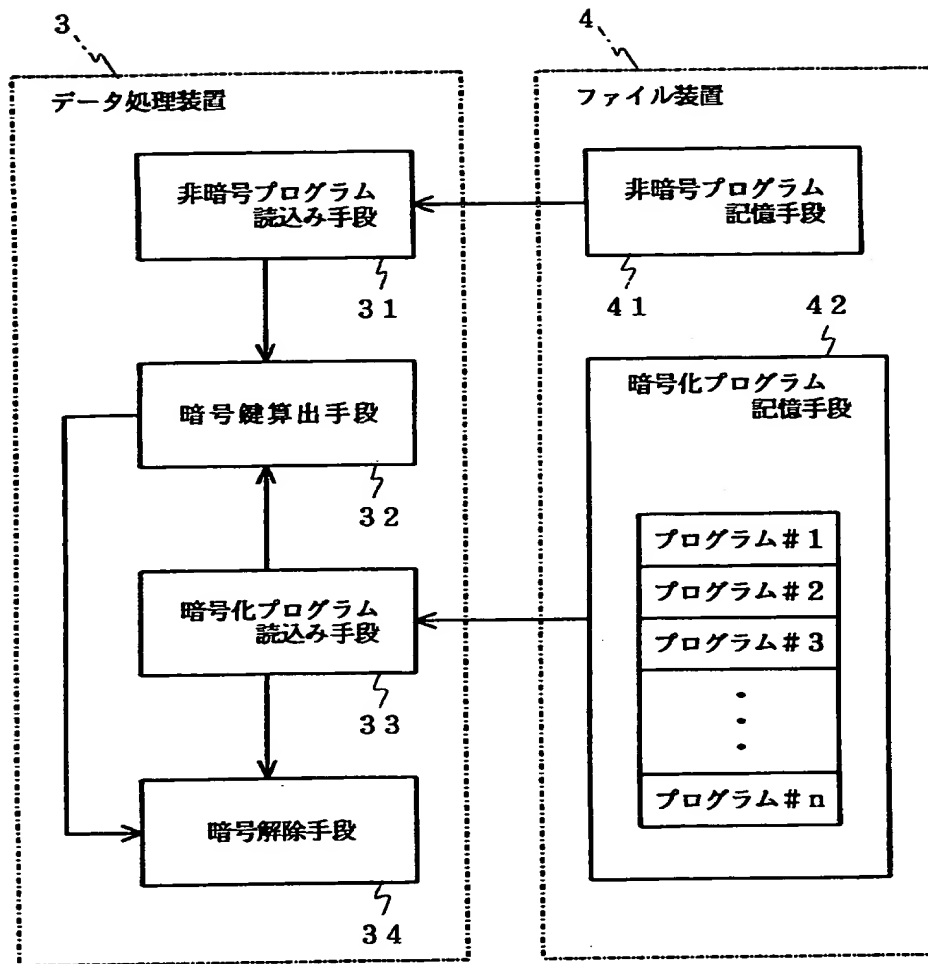
【図 2】



【図 3】



【図 4】



【書類名】 要約書

【要約】

【課題】 暗号化されたプログラムコードを高速に実行可能なプログラムコードの不正改竄防止システムを提供する。

【解決手段】 高速暗号解除手段 1 6 はデータ処理装置 1 の実行時に、データ処理装置 1 の初期化時に実行される暗号解除手段 1 4 と同様に、暗号鍵算出手段 1 2 が算出した暗号鍵を使用して暗号化されたプログラムコードの暗号を解除するが、暗号解除手段 1 4 よりも高速に暗号解除を実行する。不正操作検出手段 1 5 はソフトウェアデバッガ等によってプログラムコードの動作が解析されていないかどうかを検出する。データ処理装置 1 は不正操作検出手段 1 5 がプログラムコードの解析が行われていると判定した場合、以降の処理で暗号化されたプログラムコードを使用せずに暗号化されたダミープログラムを使用するかあるいは処理を中止する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 4 2 3 7 ]

1. 変更年月日	1 9 9 0 年 8 月 2 9 日
[変更理由]	新規登録
住 所	東京都港区芝五丁目 7 番 1 号
氏 名	日本電気株式会社